

#2

BOX PATENT APPLICATION  
Attorney Docket No. 24673

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Toshio KUROIWA

Serial No. NOT YET ASSIGNED

Filed: June 4, 2001

For: MASTER DIGITAL DATA CREATION DEVICE AND DIGITAL  
DATA REPRODUCTION DEVICE

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner of Patents  
Washington, D.C. 20231

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date June 6, 2000, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2000-168613.

A Certified Copy of the corresponding applications are submitted herewith.

Respectfully submitted,

NATH & ASSOCIATES PLLC

Date: June 4, 2001

By: Gary M. Nath

Gary M. Nath  
Reg. No. 26,965  
Customer No. 20529

NATH & ASSOCIATES PLLC  
6<sup>TH</sup> Floor  
1030 15<sup>th</sup> Street, N.W.  
Washington, D.C. 20005  
(202)-775-8383  
GMN/lis(Priority)

JC903 U.S. PTO  
09/07/1905  
06/04/01

#2

**PATENT OFFICE  
JAPANESE GOVERNMENT**

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: June 6, 2000

Application Number: P2000-168613

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

March 23, 2001

Commissioner,  
Patent Office

Kozo Oikawa

Number of Certification: 2001-3023763

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

Jc903 U.S. PRO  
09/871905  
06/04/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

2000年 6月 6日

出 願 番 号

Application Number:

特願2000-168613

出 願 人

Applicant (s):

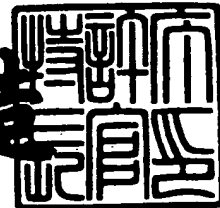
日本ビクター株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 3月23日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出願番号 出願特 2001-3023763

【書類名】 特許願

【整理番号】 411001309

【提出日】 平成12年 6月 6日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06F 17/60  
G06F 1/00  
G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 黒岩 俊夫

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守随 武雄

【代理人】

【識別番号】 100085235

【弁理士】

【氏名又は名称】 松浦 兼行

【手数料の表示】

【予納台帳番号】 031886

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コントロールワード暗号化装置及びコントロールワード復号装置

【特許請求の範囲】

【請求項 1】 指定された再生許可回数に応じて暗号化された第 1 のコントロールワードを、一方向性関数によって置換することを繰り返すことにより、置換回数が前記再生回数である第 2 のコントロールワードを生成する暗号化手段と

、  
 所望の第 1 のデジタル情報を、暗号化された前記第 2 のコントロールワードでスクランブルして得た第 2 のデジタル情報を出力するスクランブル手段と、

前記第 2 のデジタル情報と前記第 1 のコントロールワードとを外部に出力する出力手段と

を有することを特徴とするコントロールワード暗号化装置。

【請求項 2】 第 1 のコントロールワードCW<sub>k</sub>を k 回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第 2 のコントロールワードCW<sub>0</sub>で、所望の第 1 のデジタル情報をスクランブルして得た第 2 のデジタル情報が、前記第 1 のコントロールワードCW<sub>k</sub>と共に記録された記録媒体を再生することにより、前記第 2 のデジタル情報と前記第 1 のコントロールワードCW<sub>k</sub>が入力され、前記第 1 のコントロールワードCW<sub>k</sub>を前記一方向性関数によって、再帰的に k 回復号して前記第 2 のコントロールワードCW<sub>0</sub>を復号する復号化ブロックと、

前記復号化ブロックにより復号化された前記第 2 のコントロールワードCW<sub>0</sub>で、前記記録媒体から再生した前記第 2 のデジタル情報をデスクランブルして、前記第 1 のデジタル情報を出力するデスクランブラと、

入力された前記第 1 のコントロールワードCW<sub>k</sub>を前記一方向性関数によって、再帰的に 1 回復号して得た第 3 のコントロールワードCW<sub>(k-1)</sub>を前記記録媒体に書き戻して、前記第 1 のコントロールワードCW<sub>k</sub>をCW<sub>(k-1)</sub>に更新する書き戻し手段と

を有し、前記第 3 のコントロールワードCW<sub>(k-1)</sub>が前記第 2 のコントロールワ

ードCW0となるまで前記記録媒体からの前記第2のデジタル情報の正常再生を行うことを特徴とするコントロールワード復号装置。

【請求項3】 第1のコントロールワードCWkをk回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第2のコントロールワードCW0で、所望の第1のデジタル情報をスクランブルして得た第2のデジタル情報が、前記第1のコントロールワードCWkと共に記録された記録媒体を再生することにより、前記第2のデジタル情報と前記第1のコントロールワードCWkが入力され、前記第1のコントロールワードCWkを前記一方向性関数によって、再帰的にk回復号して前記第2のコントロールワードCW0を復号する復号化ブロックと、

前記復号化ブロックにより復号化された前記第2のコントロールワードCW0で、前記記録媒体から再生した前記第2のデジタル情報をデスクランブルして、前記第1のデジタル情報を出力するデスクランブラと、

他の再生装置からの再生回数nを前記復号化ブロックに入力することにより、前記第1のコントロールワードCWkを前記一方向性関数によって、 $k \geq n$ のときは再帰的に $(k - n)$ 回復号させて得られ、 $k < n$ のときは復号せずにCWkのまま得られた第3のコントロールワードCWnと、 $k \geq n$ のときは再帰的にn回復号させて得られ、 $k < n$ のときは再帰的にk回復号させてCW0として得られた第4のコントロールワードCW(k-n)をそれぞれ前記復号化ブロックから出力させると共に、前記第3のコントロールワードCWnを前記第2のデジタル情報と共に前記他の再生装置へ出力させる出力ブロックと、

前記復号化ブロックからの前記第4のコントロールワードCW(k-n)を前記記録媒体に書き戻して、前記第1のコントロールワードCWkをCW(k-n)に更新する書き戻し手段と

を有し、前記第4のコントロールワードCW(k-n)が前記第2のコントロールワードCW0となるまで前記記録媒体からの前記第2のデジタル情報の正常再生を行うことを特徴とするコントロールワード復号装置。

【発明の詳細な説明】

【0001】

## 【発明の属する技術分野】

本発明はコントロールワード暗号化装置及びコントロールワード復号装置に係り、特に配布されたオーディオデータやビデオデータ等のデジタル情報を不正に再生あるいはコピーされることを防止するコントロールワード暗号化装置及びコントロールワード復号装置に関する。

## 【0002】

## 【従来の技術】

近年、記録再生機器及びこれらに使用される媒体のデジタル化が進行し、オーディオやビデオを楽しむユーザにとっては、高速で劣化の無い記録、安定した再生等、数多くの恩恵を受けている。この反面、劣化の無いコピーが短時間で多数作製され、権利者に無許可で販売されてしまうという問題が大きくクローズアップされており、不正なコピーの防止対策が重要になっている。

## 【0003】

上記の不正なコピーを防止する手段として、例えば、デジタルオーディオテープレコーダ（DAT）やミニディスク（MD）等の従来のデジタル記録再生機器ではSCMS（Serial Copy Management System）を用いている。SCMSにおいては、媒体上の特定の領域にコピー許可状態を示す情報が記録される。すなわち、コピー元媒体に記録されているコピー許可状態を示す情報が”00”の場合は、コピー先の媒体においてもコピー許可状態を示す情報が同じ”00”で記録され、コピー先媒体からのコピーが許可される（いわゆるコピーフリー）。

## 【0004】

また、コピー元媒体に記録されているコピー許可状態を示す情報が”10”の場合は、コピー先の媒体においてはコピー許可状態を示す情報が”11”に変更して記録され、コピー先媒体からのコピーが許可されない（すなわち、1回のみコピー可）。これはSCMSに準拠する機器が、媒体上のコピー許可状態を示す情報”11”を検出したときには、コピー動作を停止するように構成されていることを前提として成立している。

## 【0005】

その他の従来のコピー防止方法の例として、デジタル情報の暗号化が挙げら

れる。これはコピー保護を行いたいデジタル情報に対して、所定のコントロールワードを用いてスクランブルを施すと共に、コントロールワードを特定のキーデータを用いて暗号化して記録するものである。

#### 【 0 0 0 6 】

図 4 は従来のコピー防止方法の一例の概略説明図を示す。同図において、マスタリング装置 1 において、例えばオーディオ等のサービスを行うためのデジタル情報 P は、スクランブラ 2 内でコントロールワード P を用いてスクランブルされ、記録媒体 4 へ出力される。と同時に、コントロールワード P は暗号化部 3 内でキーデータ K を用いて暗号化され、コントロールワード C として記録媒体 4 に出力される。

#### 【 0 0 0 7 】

再生機器 5 側では記録媒体 4 から再生したコントロールワード C を復号化部 6 に入力し、キーデータ K を用いてコントロールワード P へ復号を行う。同時に、再生機器 5 は記録媒体 4 から再生したデジタル情報 C をデスクランブラ 7 へ入力し、既に復号化部 6 で得られているコントロールワード P を用いてデジタル情報 P を得る。これら処理に好適なアルゴリズムとしては、D E S (Data Encryption Standard)、R S A 等が挙げられる。この記録媒体 4 をコピー元とするコピー操作にあたっては、デジタル情報 C のみがコピーされるため、コピー先媒体を再生する場合、デスクランブル処理を正常に実行できないためサービスを受けることができない（デジタル情報 P を正常に再生することができない）。このようにして、実質的にコピーを防止することができる。

#### 【 0 0 0 8 】

##### 【発明が解決しようとする課題】

しかしながら、SCMS の場合、コピー許可状態を示す情報が故意に書き換えられる所謂改竄が行われた場合、例えばコピー元媒体のコピー許可状態を示す情報が " 1 0 " であっても、コピー先媒体に記録する際、あるいは伝送路に処理装置を挟み込む形でコピー許可状態を示す情報を " 0 0 " に書き換える操作によって、以降の不正なコピーを許容してしまうという欠点がある。

#### 【 0 0 0 9 】



また、デジタル情報にスクランブルを施す従来方法では、画一的にコピーを阻止するために、例えばユーザが、万が一記録媒体を壊してしまう事故に備えて個人用のバックアップを作製するというような作業すら許容しない。この事はデジタル化のメリットと相反するものであり、合理的とはいえない。本来ならば、コピーという行為自体を制限するのではなく、デジタル情報を再生する、つまり、ユーザがサービスを受ける事柄に対してデジタル情報の内容の権利者は対価を求めるべきである。この事は上記のようなコピー管理方式とは異なった方法が必要であることを意味する。

#### 【 0 0 1 0 】

そこで、従来より、ユーザのデジタルコンテンツの再生操作に対して課金し、この利用金額情報を集計した後に権利者に対価の分配を与えることにより、上記の問題を解決する方法が開示されている（特開平 1 0 - 2 6 9 2 8 9 号公報：発明の名称「デジタルコンテンツ配付管理方法、デジタルコンテンツ再生方法及び装置」）。

#### 【 0 0 1 1 】

しかしながら、この従来方法及び装置では、再生機器でのデジタルコンテンツの使用状況を課金管理元に反映するために、再生機器と課金管理元の間で通信が必要であり、処理が複雑であるという問題がある。

#### 【 0 0 1 2 】

本発明は以上の点に鑑みなされたもので、再生機器と課金管理元との間で通信することなく、不正コピーを有効に防止し得るコントロールワード暗号化装置及びコントロールワード復号装置を提供することを目的とする。

#### 【 0 0 1 3 】

##### 【課題を解決するための手段】

上記の目的を達成するため、本発明のコントロールワード暗号化装置は、指定された再生許可回数に応じて暗号化された第 1 のコントロールワードを、一方向性関数によって置換することを繰り返すことにより、置換回数が再生回数である第 2 のコントロールワードを生成する暗号化手段と、所望の第 1 のデジタル情報を、暗号化された第 2 のコントロールワードでスクランブルして得た第 2 のデ

ィジタル情報を入力するスクランブル手段と、第2のディジタル情報と第1のコントロールワードとを外部に出力する出力手段とを有することを特徴とする。この発明では、第2のディジタル情報の再生回数を第2のコントロールワードの置換回数の値に予め制限することができる。

## 【 0 0 1 4 】

また、本発明のコントロールワード復号装置は、上記の目的を達成するため、第1のコントロールワードCW<sub>k</sub>をk回、一方向性関数で置換することを繰り返して得られるコントロールワードに相当する第2のコントロールワードCW<sub>0</sub>で、所望の第1のディジタル情報をスクランブルして得た第2のディジタル情報が、第1のコントロールワードCW<sub>k</sub>と共に記録された記録媒体を再生することにより、第2のディジタル情報と第1のコントロールワードCW<sub>k</sub>が入力され、第1のコントロールワードCW<sub>k</sub>を一方向性関数によって、再帰的にk回復号して第2のコントロールワードCW<sub>0</sub>を復号する復号化ブロックと、復号化ブロックにより復号化された第2のコントロールワードCW<sub>0</sub>で、記録媒体から再生した第2のディジタル情報をデスクランブルして、第1のディジタル情報を入力するデスクランブラと、入力された第1のコントロールワードCW<sub>k</sub>を一方向性関数によって、再帰的に1回復号して得た第3のコントロールワードCW<sub>(k-1)</sub>を記録媒体に書き戻して、第1のコントロールワードCW<sub>k</sub>をCW<sub>(k-1)</sub>に更新する書き戻し手段とを有する構成としたものである。この発明では、第3のコントロールワードCW<sub>(k-1)</sub>が第2のコントロールワードCW<sub>0</sub>になるまで記録媒体からの第2のディジタル情報の正常再生ができる。

## 【 0 0 1 5 】

また、本発明装置は上記の目的を達成するため、第1のコントロールワードCW<sub>k</sub>をk回、一方向性関数で置換することを繰り返して得られルコントロールワードに相当する第2のコントロールワードCW<sub>0</sub>で、所望の第1のディジタル情報をスクランブルして得た第2のディジタル情報が、第1のコントロールワードCW<sub>k</sub>と共に記録された記録媒体を再生することにより、第2のディジタル情報と第1のコントロールワードCW<sub>k</sub>が入力され、第1のコントロールワードCW<sub>k</sub>を一方向性関数によって、再帰的にk回復号して第2のコントロールワードCW<sub>0</sub>を復号する

復号化ブロックと、復号化ブロックにより復号化された第2のコントロールワードCW0で、記録媒体から再生した第2のデジタル情報をデスクランブルして、第1のデジタル情報を出力するデスクランブラと、他の再生装置からの再生回数 $n$ を復号化ブロックに入力することにより、第1のコントロールワードCW $k$ を一方方向性関数によって、 $k \geq n$ のときは再帰的に $(k - n)$ 回復号させて得られ、 $k < n$ のときは復号せずにCW $k$ のまま得られた第3のコントロールワードCW $n$ と、 $k \geq n$ のときは再帰的に $n$ 回復号させて得られ、 $k < n$ のときは再帰的に $k$ 回復号させてCW0として得られた第4のコントロールワードCW $(k - n)$ をそれぞれ復号化ブロックから出力させると共に、第3のコントロールワードCW $n$ を第2のデジタル情報と共に他の再生装置へ出力させる出力ブロックと、復号化ブロックからの第4のコントロールワードCW $(k - n)$ を記録媒体に書き戻して、第1のコントロールワードCW $k$ をCW $(k - n)$ に更新する書き戻し手段とを有する構成としたものである。

#### 【0016】

この発明では、第4のコントロールワードCW $(k - 1)$ が第2のコントロールワードCW0になるまで、記録媒体からの第2のデジタル情報の正常再生が許容されるが、他の再生装置からの再生回数 $n$ が指定されたときには、第3のコントロールワードCW $n$ を第2のデジタル情報と共に他の再生装置へ出力させると共に、第1のコントロールワードCW $k$ をCW $(k - n)$ に更新するようにしているため、制限された再生回数 $k$ はコピー操作によってコピー元からコピー先の他の再生装置へ分け与えられ、コピー元あるいはコピー先の他の再生装置でのデジタル情報の再生時に独立した再生回数管理が行われる。

#### 【0017】

#### 【発明の実施の形態】

次に、本発明の実施の形態について図面と共に説明する。図1(a)は本発明になるコントロールワード復号装置の一実施の形態のブロック図、同図(b)は同図(a)中の復号化ブロックの一例の構成図を示す。ここで、本実施の形態のコントロールワード復号装置について説明する前に、まず、本発明の不正コピー防止システムにおいて、全てのコピーの元になるデジタル情報の制作について

説明する。以降、これをマスターと呼ぶ。

【 0 0 1 8 】

図 2 は本発明のコントロールワード暗号化装置の一実施の形態のブロック図を示す。同図において、マスター制作装置 1 0 は図 2 に示すように、サービス内容であるデジタル情報のスクランブラ 2 1 と、コントロールワードの暗号化ブロック 2 2 及びユーザ側の再生装置との通信を行う通信ブロック 2 3 によって構成される。通信ブロック 2 3 は、伝送媒体 2 4 を介して再生装置 2 5 と接続可能な構成とされている。

【 0 0 1 9 】

次に、図 2 のマスター制作動作について説明する。マスター制作装置 2 0 は例えば、ユーザに映像ソフトその他のソフトを提供する店舗に置かれている。ユーザはこの店舗に出向いていき、自らの再生装置 2 5 を伝送媒体 2 4 を介してマスター制作装置 2 0 と接続する。そして、このユーザからは所望のサービスに対応するデジタル情報の指定と再生回数  $p$  が提示され、ここには図示しないが、この再生回数  $p$  に応じた課金額がユーザに対して課金される。なお、課金額はデジタル情報の種類などによっても変わる。

【 0 0 2 0 】

再生回数  $p$  は伝送媒体 2 4 とマスター制作装置 2 0 内の通信ブロック 2 3 を経由して暗号化ブロック 2 2 へ入力される。暗号化ブロック 2 2 への入力として必須ではないが、ここでは、著作権保護をより強固なものとするために、暗号化ブロック 2 2 にはキーデータ  $K$  も入力される。

【 0 0 2 1 】

キーデータ  $K$  が暗号化ブロック 2 2 に入力される場合、再生装置 2 5 側にも同一のキーデータ  $K$  が設定されていることが必要になる。キーデータ  $K$  は暗号化ブロック 2 2 内の一方方向性関数の入力として用いることができる。暗号化ブロック 2 2 の出力は、再生回数  $p$  に応じたコントロールワード  $CW_p$  と、スクランブラ 2 1 に入力されるコントロールワード  $CW_0$  がある。コントロールワード  $CW_p$  は通信ブロック 2 3 及び伝送媒体 2 4 を通じて再生装置 2 5 へ送信される。

【 0 0 2 2 】

スクランブラ 2 1 は、ユーザの要求に応じて選択されたデジタル情報 P をコントロールワード CW0 を用いてスクランブルする。スクランブル処理は DES 等の暗号化アルゴリズムが使用可能である。マスターであるスクランブラ 2 1 から出力されたデジタル情報 C は、通信ブロック 2 3 及び伝送媒体 2 4 を通じて再生装置 2 5 へ送信される。デジタル情報 C 及びコントロールワード CWp は再生装置 2 5 内の記録媒体に記録される。このようにして、ユーザが有する再生装置 2 5 には、ユーザの希望するデジタル情報 P が、スクランブルされた状態でコントロールワード CWp と共に記録された、再生回数 p だけ再生可能な記録済み記録媒体が制作される。

## 【 0 0 2 3 】

図 3 ( a ) は上記の暗号化ブロック 2 2 の一例の概略ブロック図を示す。この暗号化ブロック 2 2 は、最初にランダム値発生部 2 2 1 によりランダム値を発生し、置換操作を行う。この図 3 ( a ) の例では、再生回数 p が「 3 」であるので、図 3 ( b ) に示されるコントロールワード CW の形式に従ってランダム値の一部が値「 3 」に置換される。この結果をコントロールワード CW3 として出力する。

## 【 0 0 2 4 】

ここで、コントロールワード CW は、図 3 ( b ) にフォーマット例を示すように、一方向性関数 f のランダム値 2 7 と置換値 2 8 とからなる。置換値 2 8 はコントロールワード CW0 を得るまでの一方向性関数 f の適用回数を示す。これは、コントロールワード復号装置内でデジタル情報の再生権利をすべて使い切ったか、あるいはデジタル情報のデスクランブルに必要なコントロールワードを得たことを認識するために用いられる、コントロールワード CW0 を得るまでの一方向性関数の適用回数である。

## 【 0 0 2 5 】

上記のコントロールワード CW3 は、更に再生回数分だけ一方向性関数 f によって再帰的に処理される。一方向性関数 f は、出力から入力を推測することが困難である関数と定義される。必要ならば、キーデータ K はコントロールワード CW と共に一方向性関数 f へ入力される。各段の一方向性関数 f の出力は、同様の置換操作を受け、最終的にコントロールワードの一部が 0 となった状態で CW0 として出

力される。このコントロールワードCW0がスクランブラ21に用いられる。

【0026】

次に、図1に戻って本発明装置の一実施の形態について説明する。図1(a)において、再生装置10は、伝送媒体16を通じて他の再生装置17に接続されており、図2に示した再生装置25を用い得る。再生装置10は、記録媒体11a及び11b、復号化ブロック12、デスクランブラ13、再生部14及び通信ブロック15とから構成されている。記録媒体11aには、前述したマスター制作装置20からの、ユーザの希望するデジタル情報Pがスクランブルされた状態の情報Cが記録されており、また、記録媒体11bにはコントロールワードCW<sub>p</sub>が記録されている。

【0027】

デスクランブラ13は復号化ブロック12からのコントロールワードCW0を用いて記録媒体11aからのデジタル情報をデスクランブルしてデジタル情報Pを得る。再生部14は入力デジタル情報Pを再生する。通信ブロック15は、復号化ブロック12と他の再生装置17との間で伝送媒体16を介して通信するために設けられている。

【0028】

復号化ブロック12は図1(b)のブロック図に示すように、内部に記録媒体11bから読み出したコントロールワードCW<sub>k</sub>を一時記憶するCW<sub>k</sub>レジスタ121と、通信ブロック15へ出力するコントロールワードを一時記憶するCW<sub>n</sub>レジスタ122と、デスクランブラ13へ出力するコントロールワードCW0を一時記憶するCW0レジスタ123と、一方向性関数f置換処理部124とより構成されており、一方向性関数f置換処理部124には再生回数nが他の再生装置17から入力される。

【0029】

次に、図1(a)及び(b)の実施の形態の動作について説明する。マスター制作装置20でコントロールワードCW0を用いてスクランブルされた、例えばオーディオ等のサービスを行うためのデジタル情報Cは、再生装置10に入力されて内蔵の記録媒体11aに記録され、また、これと同時に再生回数pに応じたコン

トロールワードCW<sub>p</sub>が入力されて再生装置10に内蔵された記録媒体11bに記録されている。

【0030】

記録媒体11bに記録されたコントロールワードCW<sub>p</sub>は、読み出されて復号化ブロック12に供給され、ここでマスター制作装置20で用いたものと同じキーワードKを用いてコントロールワードCW<sub>0</sub>に復号化され、記録媒体11aから読み出されたデジタル情報Cと共にデスクランブラ13に入力される。デスクランブラ13は、入力されたデジタル情報Cを、復号コントロールワードCW<sub>0</sub>を用いてデスクランブル処理を行って、デジタル情報Pを復元して再生部14に出力する。

【0031】

再生部14では、デスクランブラ13から入力されたデジタル情報Pの符号化に対応した復号化を行い、復号化したデータを再生装置10の外部へ出力してユーザにサービスを提供する。再生の終了を確認した後に、復号化ブロック12は記録媒体11bにコントロールワードCW(p-1)を書き戻す。

【0032】

次に、記録媒体11a上にあるデジタル情報Cを他の再生装置17の記録媒体へコピーする場合の動作について説明する。この場合は、まず、通信ブロック15を通じて、他の再生装置17が所望の再生回数nを再生装置10にリクエストする。現在、記録媒体11bに記録されているコントロールワードをCW<sub>k</sub>とした場合、復号化ブロック12はこのコントロールワードCW<sub>k</sub>を記録媒体11bから読み出し、一方向性関数および置換を再帰的に適用してコントロールワードCW<sub>n</sub>を出力する。

【0033】

復号化ブロック12から出力されたコントロールワードCW<sub>n</sub>は、記録媒体11aから読み出されたデジタル情報Cと共に、通信ブロック15及び伝送媒体16を通して他の再生装置17に供給され、その記録媒体にコピー記録される。正常なコピーが確認された後に、復号化ブロック12はコントロールワードCW<sub>k</sub>へ一方向性関数および置換を再帰的に適用した結果であるコントロールワードCW<sub>k</sub>'

で記録媒体 11b の内容を更新する。ここに  $k' = k - n$  なる関係がある。つまり、再生回数  $k$  だけ許容されている記録媒体 11a 及び 11b から、他の再生装置 17 の記録媒体に対して再生回数  $n$  を許容するコピー記録を行ったので、記録媒体 11a 及び 11b の再生回数は残りの  $(k - n)$  回とされる。

## 【0034】

次に、復号化ブロック 12 の処理について更に具体的に説明する。いま、記録媒体 11b に記録されているコントロールワードが CW5 である場合 ( $k = 5$ )、すなわち 5 回の再生権利を持っている場合のデジタル情報のコピーを 1 回行う場合について説明する。この場合、記録媒体 11b に記録されているコントロールワード CW5 は、復号化ブロック 12 により読み出されて復号化ブロック 12 内の CWk レジスタ 121 に一時記憶される。

## 【0035】

次に、CWk レジスタ 121 の記憶コントロールワード CW5 に対して、処理部 124 で一方向性関数  $f$  と置換を 1 回行い、この結果を CWk レジスタ 121 に記憶して記憶内容を更新する。一方向性関数  $f$  と置換処理は図 3 (a) に示した暗号化ブロック 22 内の処理と同一である。すなわち、この時点で CWk レジスタ 121 の内容は CW4 となっている。

## 【0036】

引き続き、処理部 124 により一方向性関数  $f$  と置換処理を繰り返し行い、結果が CW0 となった時点で、このコントロールワード CW0 を CW0 レジスタ 123 に記憶する。最後に、CWk レジスタ 121 の記憶内容を記録媒体 11b に書き戻し、CW0 レジスタ 123 の内容をデスクランブラ 13 に出力する。

## 【0037】

次に、記録媒体 11b に記録されているコントロールワードが CW5 である場合 ( $k = 5$ )、すなわち 5 回の再生権利を持っている場合に、再生回数「2」 ( $n = 2$ ) が指定された、デジタル情報のコピーについて説明する。この場合、記録媒体 11b に記録されているコントロールワード CW5 は、復号化ブロック 12 により読み出されて復号化ブロック 12 内の CWk レジスタ 121 に一時記憶される。

## 【0038】



ここで、再生回数「2」が指定されているので、当再生装置での再生権利数は「3」( $= 5 - 2$ )となる。従って、CWkレジスタ121に記憶されているコントロールワードCW5に、処理部124により一方向性関数fと置換処理を2回適用し、コントロールワードCW3を得て、これをCWkレジスタ121に記憶して記憶内容を更新する。

## 【0039】

更に、更新後のCWkレジスタ121のコントロールワードCW3に対して、処理部124により一方向性関数fと置換処理を1回適用し、コントロールワードCW2を得てこれをCWnレジスタ122に格納する。引き続き、処理部124により一方向性関数fと置換処理を繰り返し行い、結果がCW0となった時点で、このコントロールワードCW0をCW0レジスタ123に記憶する。最後に、CWnレジスタ122に格納されたコントロールワードCW2を通信ブロック15に出力した後に、記録媒体11bへCWkレジスタ121の内容(CW3)を書き戻す。

## 【0040】

次に、記録媒体11bに記録されているコントロールワードがCW5である場合( $k = 5$ )、すなわち5回の再生権利を持っている場合に、再生回数「6」( $n = 6$ )が指定された、デジタル情報のコピーについて説明する。この場合、記録媒体11bに記録されているコントロールワードCW5は、復号化ブロック12により読み出されて復号化ブロック12内のCWkレジスタ121に一時記憶される。

## 【0041】

ここで、指定された再生回数「6」は、当再生装置での再生権利数「5」より多いので、処理部124により一方向性関数fと置換処理を6回適用しようとしても、再生権利数に等しい5回適用した時点でコントロールワードがCW0となるため、このCW0がCWkレジスタ121とCW0レジスタ123に記憶されて記憶内容を更新する。また、それまでCWkレジスタ121に記憶されていたコントロールワードCW5がCWnレジスタ122に記憶される。

## 【0042】

最後に、CWnレジスタ122に格納されたコントロールワードCW5を通信ブロック15に出力した後に、記録媒体11bへCWkレジスタ121の内容(CW0)を書

き戻す。その後、記録媒体 1 1 a と 1 1 b の再生時には、記録媒体 1 1 b からコントロールワードとして CW0 が再生されるため、復号化ブロック 1 2 による復号化が行われず、再生が正常にできなくなる。このように、この実施の形態では、再生権利数よりも多い再生回数が指定されても、再生権利数だけのコピーのみ可能であり、再生権利数よりも多いコピーを防止することができる。

#### 【0043】

##### 【発明の効果】

以上説明したように、本発明によれば、第 3 のコントロールワードの置換回数が第 2 のコントロールワードと同じ置換回数になるまで正常な再生を可能とすることにより、第 2 のデジタル情報の再生回数を第 1 のコントロールワードの置換回数と第 2 のコントロールワードの置換回数との差の値に予め制限でき、これにより簡潔な課金管理を実現するようにしたため、デジタル情報の権利者に対する対価についての課金処理は最初の記録媒体への記録時に、ユーザの意思によって予め決めた再生回数に応じた金額を徴収することで終了させ、再生のたびに課金管理元と通信することを不要にできる。

#### 【0044】

また、本発明によれば、制限された再生回数  $k$  はコピー操作によってコピー元からコピー先の他の再生装置へ分け与えられ、コピー元あるいはコピー先の他の再生装置でのデジタル情報の再生時に独立した再生回数管理が行われるようにしたため、一方向性関数の性質によりコピー時にも再生権利数に対する改竄の恐れなく処理を行うことができることと相まって、高速で劣化の無い記録、安定した再生等のデジタル化のメリットを損なうことなく、デジタル情報の配布ができると共に不正コピーを防止できる。

##### 【図面の簡単な説明】

#### 【図 1】

本発明装置の一実施の形態のブロック図と要部の構成図である。

#### 【図 2】

本発明暗号化装置の一実施の形態のブロック図である。

#### 【図 3】

図 2 の暗号化ブロックの一例の説明図とコントロールワードの形式を示す図である。

【図 4】

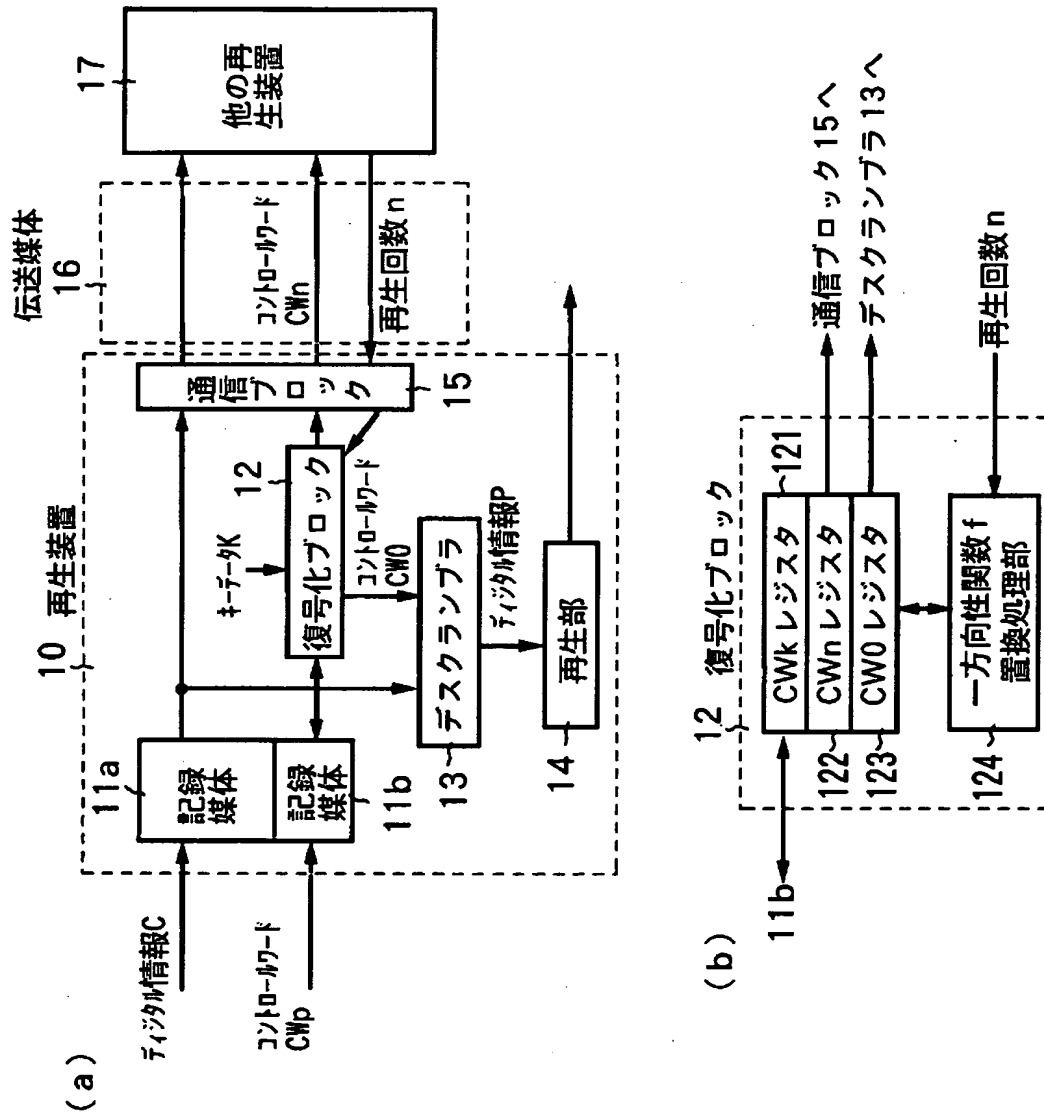
従来のコピー防止方法の一例の概略説明図である。

【符号の説明】

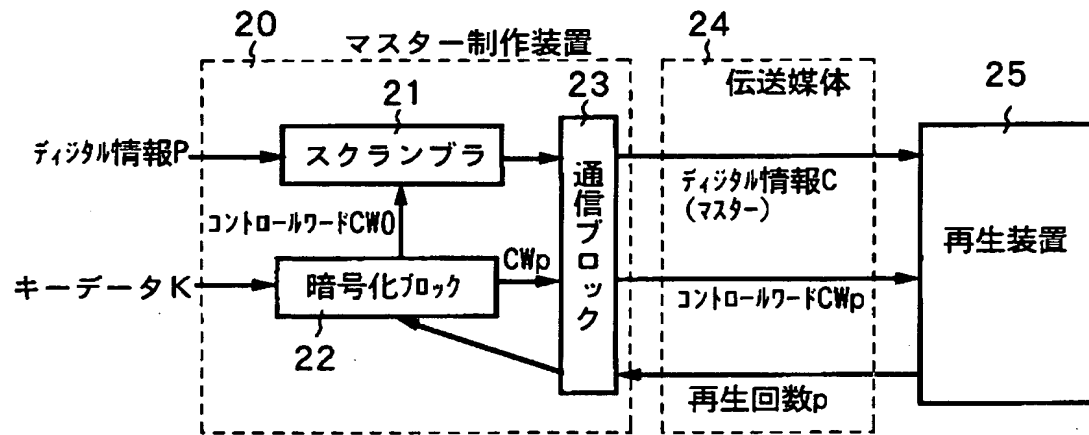
- 1 0、2 5 再生装置
- 1 1 a、1 1 b 記録媒体
- 1 2 復号化ブロック
- 1 3 デスクランブラ
- 1 4 再生部
- 1 5、2 3 通信ブロック
- 1 6、2 4 伝送媒体
- 1 7 他の再生装置
- 2 0 マスター制作装置
- 2 1 スクランブラ
- 2 2 暗号化ブロック
- 1 2 1 CWkレジスタ
- 1 2 2 CWnレジスタ
- 1 2 3 CW0レジスタ
- 1 2 4 一方向性関数 f 置換処理部
- 2 2 1 ランダム値発生部

【書類名】 図面

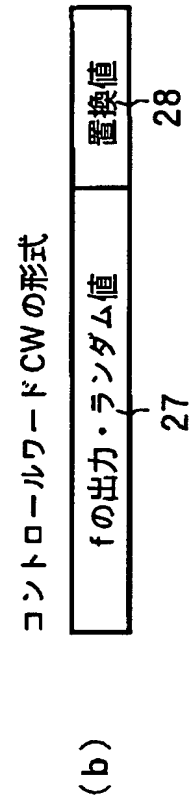
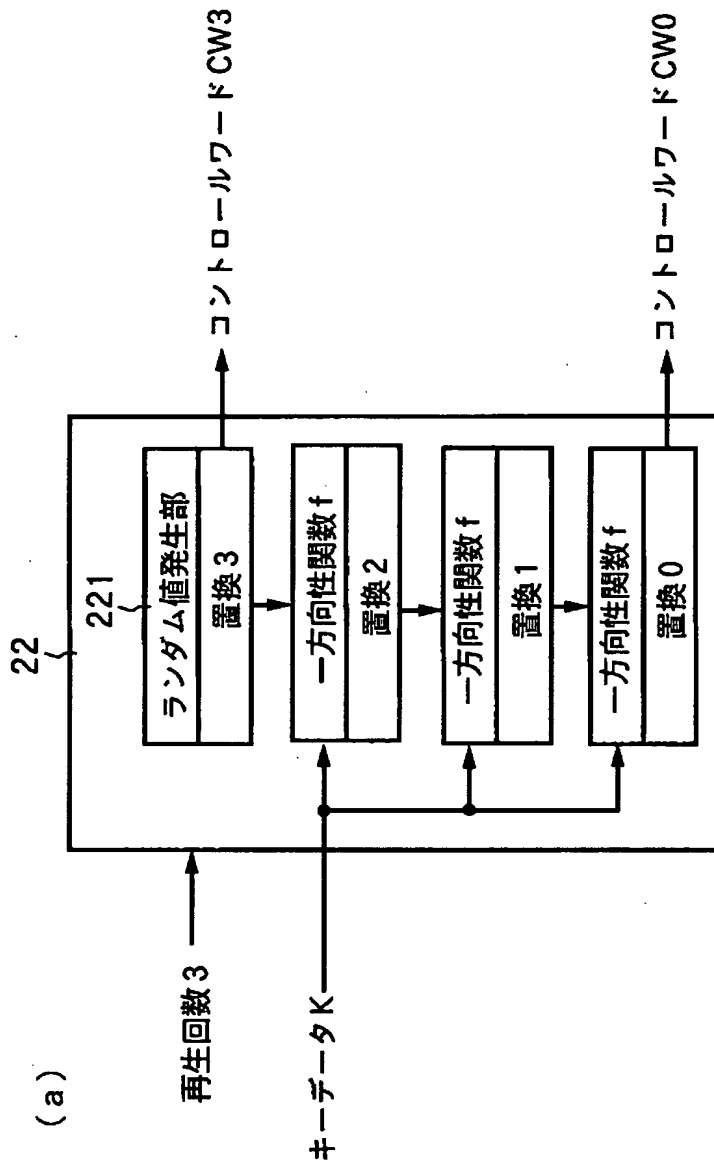
【図 1】



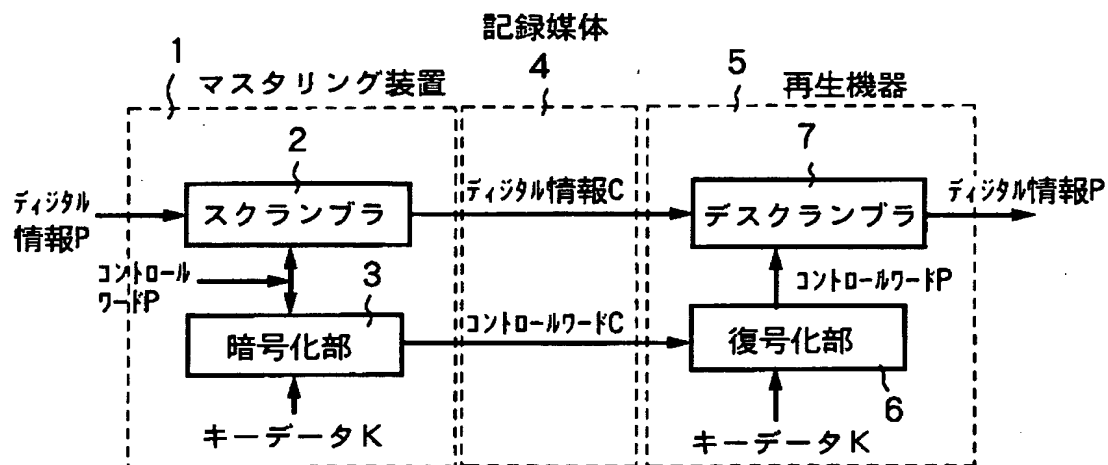
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 従来は、再生機器でのコンテンツの使用状況を課金管理元に反映するために、再生機器と課金管理元の間で通信が必要であり、処理が複雑である。

【解決手段】 記録媒体 1 1 a には、ユーザの希望するデジタル情報 P がスクランブルされた状態の情報 C が記録されており、記録媒体 1 1 b には再生回数 p に対応するコントロールワード CW<sub>p</sub> が記録されている。マスター制作時に、再生回数 p に応じてユーザに対して課金が終わっている。復号化ブロック 1 2 は、記録媒体 1 1 b からのコントロールワード CW<sub>p</sub> を CW<sub>0</sub> に復号化する。デスクランブラ 1 3 は、復号コントロールワード CW<sub>0</sub> を用いてデジタル情報 P を復元して再生部 1 4 に出力する。再生の終了を確認した後に、復号化ブロック 1 2 は記録媒体 1 1 b にコントロールワード CW(p-1) を書き戻す。再生機器と課金管理元の間で通信を行うことなく、記録媒体 1 1 a 及び 1 1 b は p 回再生可能である。

【選択図】 図 1



出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日	1990年 8月 8日
[変更理由]	新規登録
住 所	神奈川県横浜市神奈川区守屋町3丁目12番地
氏 名	日本ビクター株式会社